Dell Data Protection | Enterprise Edition for Mac

Administrator Guide

© 2013 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, Skydrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

2013-10

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

1 Introduction 5

Overview **5**

Customer Support **5**

2 Requirements 7

Hardware **7**

Software **7**

3 Tasks 9

Install/Upgrade Dell Data Protection | Enterprise Edition for Mac **9**

Prerequisites 9

Interactive Installation/Upgrade and Activation 10

Activate Dell Data Protection | Enterprise Edition for Mac **11**

Command Line Installation/Upgrade 12

Enable Encryption **15**

View Encryption Policy and Status **16**

View Policy and Status on the Local Computer 16

View Policy and Status in the Dell Remote Management Console 21

User Experience **22**

Recovery **22**

Mount Volume 23

Accept New System Configuration 24

FileVault Recovery 25

Uninstall Dell Data Protection | Enterprise Edition for Mac **27**

4 Activation as Administrator 29

Activate **29**

Activate Temporarily **29**

Appendix A 31

About Optional Firmware Password Protection **31**

Appendix B 33

How to Enable Mac OS X Boot Camp **33**

Appendix C 35

How to Retrieve a Firmware Password **35**

Appendix D 37

Client Tool **37**

Glossary 39

1

Introduction

The Dell Data Protection | Enterprise Edition for Mac Administrator Guide provides the information needed to deploy and install the client software.

Overview

Dell enables an enterprise to support a mobile workforce with the peace of mind that sensitive information is secure.

- Dell Data Protection | Enterprise Edition for Mac - client software that encrypts all data and enforces access control
- Dell Policy Proxy - used to distribute policies
- Dell Device Server - used for client software activations
- Dell Enterprise Server - provides centralized security policy administration, integrates with existing enterprise directories and creates audit logs and reports

These Dell components inter-operate seamlessly to provide a secure mobile environment without detracting from the user experience.

Customer Support

Refer to your Welcome Letter for Dell Pro Support contact information.

When contacting Dell Pro Support, have the following information available:

- For the Dell Enterprise Server, the version number can be found in the About link in the Dell Remote Management Console.
- For the client software, the version number can be found in System Preferences.

  Open Dell Data Protection preferences to see the version number in the bottom, right side of the pane.
- Operating system version for the server/workstation where the relevant components are running.
- A detailed description of the issue you are experiencing.
- Information about where we can reach you.

2

Requirements

Client hardware and software requirements are provided in this chapter. Ensure that the deployment environment meets the requirements before continuing with deployment tasks.

Hardware

The following table details supported hardware.

NOTE: The system disk must be partitioned with the GUID Partition Table (GPT) partition scheme and have a Mac OS X Extended (Journaled) format.

Hardware
• Intel-x86 processor
• 512 MB RAM
• 30 MB of free disk space
• 10/100/1000 or Wi-Fi network interface card
• Fusion Drive with a solid state drive and a hard disk drive (Requires Mac OSX 10.8 Mountain Lion or later)

Software

The following table details supported software.

NOTE: If you intend to perform a major operating system upgrade, such as from Lion to Mountain Lion, a decrypt and uninstall operation will be needed, followed by regular installation of Dell Data Protection | Enterprise Edition for Mac on the new operating system.

Operating Systems (32- and 64-bit kernels)
• Mac OS X Lion 10.7.5
• Mac OS X Mountain Lion 10.8.3, 10.8.4, and 10.8.5
• Mac OS X Mavericks 10.9

The following table details the operating systems supported when accessing encrypted external media.

NOTE: Formats supported for external media include exFAT format on flash drives, FAT32 formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes.

NOTE: External media must have 20MB available, plus open space on the media that is equal to the largest file to be encrypted, to host External Media Edition.

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media
• Microsoft Windows XP SP3
- Professional Edition
- Home Edition
- Media Center Edition
- Tablet PC Edition

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional - Ultimate - Home Premium
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer)
Mac Operating Systems (32- and 64-bit kernels) Supported to Access Encrypted Media
• Mac OS X Lion 10.7.5
• Mac OS X Mountain Lion 10.8.3, 10.8.4, and 10.8.5
• Mac OS X Mavericks 10.9

3

Tasks

Install/Upgrade Dell Data Protection | Enterprise Edition for Mac

This section guides you through the Dell Data Protection | Enterprise Edition for Mac installation/upgrade and activation process.

There are two methods to install/upgrade Dell Data Protection | Enterprise Edition for Mac. Select **one** of the following:

- Interactive Installation/Upgrade and Activation - This method is the easiest method to install or upgrade the client software package. However, this method does not allow any customizations. If you intend to use Boot Camp or a version of operating system that is not yet fully supported by Dell (see **Note** below), you must use the command line installation/upgrade method.
- Command Line Installation/Upgrade - This is an advanced installation/upgrade method that should only be used by administrators experienced with command line syntax. If you intend to use Boot Camp or a version of operating system that is not yet fully supported by Dell (see **Note** below), you must use this method to install or upgrade the client software package.

  For more information on the Installer Command options, see the Mac OS X Reference Library at http://developer.apple.com. Dell highly recommends using remote deployment tools, such as Apple Remote Desktop, to distribute the client installation package.

NOTE: Apple often releases new versions of operating systems in between releases of Dell Data Protection | Enterprise Edition for Mac. To support as many customers as possible, we allow a modification of the com.dell.ddpe.plist file to support these cases. As soon as Apple releases a new version, we begin testing these versions to ensure that they are compatible with Dell Data Protection | Enterprise Edition for Mac.

Prerequisites

Dell recommends that IT best practices are followed during the deployment of client software. This includes, but is not limited to, controlled test environments for initial tests and staggered deployments to users.

Before beginning this process, ensure the following prerequisites are met:

- Ensure that the Dell Enterprise Server and its components are already installed. If not, follow the instructions in the *Enterprise Server Installation and Migration Guide* and then return to this document for instructions to install the client software.
- Ensure that you have the Dell Device Server and Dell Policy Proxy URLs handy. Both will be needed for client software installation and activation.
- If your Dell enterprise deployment uses a non-default configuration, ensure that you have your port number for the Dell Device Server handy. It will be needed for client software installation and activation.
- Ensure that the target computer has network connectivity to the Dell Device Server and Dell Policy Proxy.
- Ensure that you have a domain user account in the Active Directory installation configured for use with the Dell Enterprise Server. The domain user account will be used for client software activation. Configuring Mac OS X for domain (network) authentication is not required.
- If you want policies to take effect immediately after client software installation, turn the *Allow Activations* policy in the Dell Remote Management Console to *True*.

Interactive Installation/Upgrade and Activation

To install/upgrade and activate the client software, follow the steps below. You must have an administrator account to perform these steps.

NOTE: Before you begin, save the user's work and close other applications; immediately after the installation is complete, the computer will need to restart.

1. Open the Dell-Data-Protection-<version>.dmg file located in the Dell installation media and open the installer. The following message displays: *This package will run a program to determine if the software can be installed.*
2. Click **Continue** to proceed.
3. Read the Welcome text and click **Continue**.
4. Review the license agreement, click **Continue**, and then click **Agree** to accept the terms of the license agreement.
5. In the **Domain Address:** field, enter the fully qualified domain for the target users, such as *department.organization.com*.
6. In the **Display Name (optional):** field, consider setting the *Display Name* to the NetBIOS (pre-Windows 2000) name of the domain, which is typically in uppercase.

   If set, this field is displayed instead of the Domain Address in the *Activation* dialog. This provides consistency with the domain name shown in *Authentication* dialogs for domain managed Windows computers.
7. In the **Device Server**: field, enter the Dell Device Server host name.

   If your deployment uses a non-default configuration, update the port fields and *Use SSL* check box.

   Once a connection is established, the Dell Device Server connectivity indicator changes from red to green.
8. In the **Policy Proxy:** field, the Dell Policy Proxy host name is auto-populated with a Dell Policy Proxy host that matches the Dell Device Server host. This host is used as the Dell Policy Proxy if no hosts are specified in the policy configuration.

   After a connection is established, the Dell Policy Proxy connectivity indicator changes from red to green.
9. Once the *Dell Data Protection Configuration* dialog is complete and connectivity has been established to the Dell Device Server and Dell Policy Proxy, click **Continue** to show the installation type.
10. Some installations on specific computers display a *Select a Destination* dialog before the *Installation Type* dialog displays. If so, select the current system disk out of the list of disks displayed. The current system disk's icon displays a green arrow pointing to the disk. Click **Continue**.
11. After the installation type displays, click **Install** to continue with the installation.
12. When prompted, enter the administrator account credentials (required by the Mac OS X Installer application), then click **OK**.

NOTE: Immediately after the installation is complete, you must restart the computer. If you have open files in other applications and are not ready to restart, click **Cancel,** save the work, and close the other applications.

13. Click **Continue Installation**. The installation begins.
14. When the installation completes, click **Restart**.

Activate Dell Data Protection | Enterprise Edition for Mac

The activation process associates network user accounts in the Dell Enterprise Server to the Mac computer and retrieves each account's security policies, sends inventory and status updates, enables recovery workflows, and provides comprehensive compliance reporting. The client software performs the activation process for each user account it finds on the computer as each user logs in to his user account.

After the client software has been installed and the Mac has restarted, the user logs in:

1. Enter the user name and password managed by Active Directory.
2. Select the Domain to log on to.
3. Click **Activate**.

   If policies have already been set in the Dell Remote Management Console and you have Encrypt Using FileVault for Mac=True, the following prompts will display. If polices have not yet been set in the Dell Remote Management Console, these prompts will display upon the *Encrypt Using FileVault for Mac=True* policy being received by the endpoint.

   a. In *Universal Access*, enable **Access for Assistive Devices**.

   b. In *Security & Privacy*, unlock **FileVault**.

      The computer will be tested using Disk Utility.

   c. Generate a unique FileVault recovery pass phrase.

      The recovery pass phrase is escrowed to the Dell Enterprise Server.

      FileVault is activated for the System Volume.

NOTE: You cannot encrypt volumes other than the System Volume if you choose the *Encrypt Using FileVault for Mac* policy. If all fixed volumes (which includes the System Volume) must be encrypted, set this policy to *False* and use the *Volumes Targeted for Encryption* policy instead.

If the Dell Enterprise Server is configured for multi-domain support and a different domain must be used for activation, use the User Principle Name (UPN), which is of the form *<username>@<domain>*.

If activation fails, the client software allows three attempts to enter correct domain credentials. If all three attempts fail, the prompt for domain credentials re-displays on the next user login.

You may also click **Not Now** to dismiss the dialog, which will re-display on the next user login.

If activation succeeds, a message for successful activation displays.

Dell Data Protection | Enterprise Edition for Mac is now fully operational and managed by the Dell Enterprise Server.

NOTE: When the administrator needs to decrypt a drive on a Mac computer that is running OS X Mountain Lion or Mavericks, whether from a remote location, by running a script, or in person, the client software will prompt the user to allow the administrator access, and will require the user to enter their password.

The remainder of this section describes command line installation. If you have just completed the interactive installation, you may skip the section called *Command Line Installation/Upgrade*. Instead, continue to Enable Encryption if encryption was **not** enabled prior to activation. If encryption **was** enabled prior to activation, continue to View Encryption Policy and Status.

Command Line Installation/Upgrade

To install the client software using the command line, follow the steps below. If you intend to use Boot Camp on encrypted Mac computers or intend to use a version of operating system that is not yet fully supported by Dell, you **must** configure your installation to **not** use firmware password protection (you must modify the com.dell.ddp.plist as shown in step 3 below.)

1. Open the Dell-Data-Protection-<version>.dmg file located in the Dell installation media.
2. Copy the **Install Dell Data Protection** package and the **com.dell.ddp.plist** file to the local drive.
3. Open the .plist file and edit the placeholder values as follows:

NOTE: Apple often releases new versions of operating systems in between releases of Dell Data Protection | Enterprise Edition for Mac. To support as many customers as possible, Dell allows a modification of the.plist file to support these cases. As soon as Apple releases a new version, Dell begins testing these versions to ensure that they are compatible with Dell Data Protection | Enterprise Edition for Mac.

NOTE: When the FirmwarePasswordMode key option is set to **Optional**, it only disables client software's enforcement of firmware password protection. It does **not** remove any existing firmware password protection. After these steps are complete, the installation is finished, and the computer restarts, you can remove any existing firmware password using the Mac OS X Firmware Password Utility.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>AllowInstallWithoutConnectivity</key>
        <false/> [Do not modify]
        <key>AllowInstallerConfigModification</key>
        <true/> [Do not modify]
        <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist file, it must be added to
        the file. Add from <key> through </array> to allow a newer version of operating system to be used. See Note
        above.]
        <array>
                <string>10.<x.x></string> [Operating system version]
        </array>
        <key>RemoveRecoveryPartition</key
        <true/> [On computers running Lion, and then overwritten by a previous Mac OS (such as Snow Leopard), the
        operating system leaves the Lion Recovery partition on the drive. Computers in this state fail to start encryption
        due to the volume failing Dell drive verification testing. When setting this value to True, on reboot of the computer,
        the Lion recovery partition will be removed, the disk verification will be successful, and encryption can begin.]
        <key>DeviceServers</key>
        <array>
                <dict>
                        <key>Host</key>
                        <string>deviceserver.organization.com</string> [Replace this value with your Dell Device Server
                        URL]
                        <key>Port</key>
    <integer>8443 or 8081</integer> [Beginning in v8.0, the default port number is 8443. However, port number 8081
    will still allow activations. In general, if your Enterprise Server is v8.0 or later, use port 8443. If your Enterprise Server is
    pre-v8.0, use port 8081.]
                        <key>UseSSL</key>
                        <true/> [We recommend a true value]
                </dict>
     </array>
```

```
    <key>Domains</key>
    <array>
        <dict>
            <key>DisplayName</key>
            <string>COMPANY</string>
            <key>Domain</key>
            <string>department.organization.com</string> [Replace this value with the Domain URL that
            users will activate against]
        </dict>
    </array>
    <key>FirmwarePasswordMode</key>
    <string>Required</string> [If using Boot Camp, this value must be Optional. For more information, see
    About Optional Firmware Password Protection.]
    <key>PolicyProxies</key>
    <array>
        <dict>
            <key>Host</key>
            <string>policyproxy.organization.com</string> [Replace this value with your Dell Policy Proxy
            URL]
            <key>Port</key>
            <integer>8000</integer> [Leave as-is unless there is a conflict with an existing port]
        </dict>
    </array>
    <key>Version</key>
    <integer>2</integer> [Do not modify]
</dict>
</plist>
```

4. Save and close the file.
5. For each targeted computer, copy the package to a temp folder and the **com.dell.ddp.plist** file to **/Library/Preferences**.
6. Perform a command line installation of the package using the **installer** command.
   `sudo installer -pkg "Install Dell Data Protection.mpkg" -target/`
7. Restart the computer using the following command line:
   `sudo shutdown -r now`

   After the client software has been installed, the computer has been restarted, and the user has logged in, the client software begins the activation process. The activation process runs once for each user account on the computer and begins when each user logs in to his unique user account. The process associates network user accounts found on the Mac computer with the accounts in the Dell Enterprise Server, and retrieves security policies, sends inventory and status updates, enables recovery workflows, and provides comprehensive compliance reporting.

   After user login, the client software prompts for domain credentials.

8 Enter the user name and password managed by Active Directory, select the Domain to log on to, and click **Activate**.

If policies have already been set in the Dell Remote Management Console and you have Encrypt Using FileVault for Mac=True, the following prompts will display. If polices have not yet been set in the Dell Remote Management Console, these prompts will display upon the *Encrypt Using FileVault for Mac=True* policy being received by the endpoint.

a In *Universal Access*, enable **Access for Assistive Devices**.

b In *Security & Privacy*, unlock **FileVault**.

The computer will be tested using Disk Utility.

c Generate a unique FileVault recovery pass phrase.

The recovery pass phrase will be escrowed to the Dell Enterprise Server.

FileVault will be activated for the System Volume.

NOTE: You cannot encrypt volumes other than the System Volume if you choose the *Encrypt Using FileVault for Mac* policy. If all fixed volumes (which includes the System Volume) must be encrypted, set this policy to *False* and use the *Volumes Targeted for Encryption policy* instead.

If the Dell Enterprise Server is configured for multi-domain support and a different domain must be used for activation, use the User Principle Name (UPN), which is of the form *<username>@<domain>*.

If activation fails, the client software allows three attempts to enter correct domain credentials. If all three attempts fail, the prompt for domain credentials re-displays on the next user login.

d You may also click **Not Now** to dismiss the dialog, which will re-display on the next user login.

If activation succeeds, a message for successful activation displays.

9 When prompted, click **Restart**.

Dell Data Protection | Enterprise Edition for Mac is now fully operational and managed by the Dell Enterprise Server.

NOTE: When the administrator needs to decrypt a drive on a Mac computer that is running OS X Mountain Lion or Mavericks, whether from a remote location, by running a script, or in person, the client software will prompt the user to allow the administrator access and will require the user to enter the password.

Continue to Enable Encryption if encryption was **not** enabled prior to activation. If encryption **was** enabled prior to activation, continue to View Encryption Policy and Status.

Enable Encryption

NOTE: Only Mac OS X Extended (Journaled) volumes and system disks that are partitioned with the GUID Partition Table (GPT) partition scheme are supported for encryption.

Use this process to enable encryption on a client computer if encryption was **not** enabled prior to activation. This process enables encryption only for a single computer. You can choose to enable encryption for all Mac computers at the *Enterprise* policy level if desired. For additional instructions about enabling encryption at the *Enterprise* policy level, see the Admin Help.

1. As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left pane, click **Protect & Manage** > **Endpoints**.
3. Enter a filter to search for the endpoint. The wild card character is *. For best results, include non-wild card characters at the beginning of the filter (e.g., User* instead of *ser). You can enter Common Name, Universal Principal Name, or sAMAccountName. You may also leave the field blank to display all endpoints.
4. Click **Search**. An endpoint or list of endpoints displays, based on your search filter.
5. Locate the appropriate endpoint and click the **Details** icon.
6. Click the **Security Policies** tab.
7. Select the **Mac Encryption** policy category.
8. Expand **General Settings**.
9. Verify that the *Encryption Enabled* policy is *True*.
10. If a Mac has a fusion drive, FileVault must be enabled to encrypt it. Verify that the *Encryption Enabled using FileVault for Mac* policy is *True*. When FileVault encryption is enabled, none of the other policies in the group will be in effect.
11. Change other policies as desired.

NOTE: See the table on page 16 for complete descriptions of each policy.

12. When finished, click **Save**.
13. In the left pane, click **Actions** > **Commit Policies**.
14. Click **Apply Changes**.
15. Wait for the policy to propagate from the Dell Enterprise Server to the Dell Policy Proxy, and then (on the target computer) click **Refresh** in the Policies pane of Dell Data Protection Preferences.

    After the client software has received the new policy, it performs a Disk Utility validation of the volumes targeted for encryption and then configures those volumes for encryption.

    This process may slow the responsiveness of the computer for a few minutes. For each volume pending encryption, a dialog displays to the user indicating the operation is taking place.

NOTE: To maintain the integrity of user data, the client software does not begin encryption on a volume until the verification process is successful on that volume. If a volume fails verification, the client software notifies the user and reports the failure in Dell Data Protection Preferences. If you need to repair a volume, follow the instructions in Apple Support article HT1782 (http://support.apple.com/kb/HT1782). The client software re-attempts verification on the next computer restart.

The client software may prompt the user to restart the computer, depending on the User Experience policies set in the Dell Remote Management Console.

The client software can begin and complete the encryption process, as well as report encryption status to the Dell Remote Management Console all before user login. This allows you to enforce compliance across all Mac computers without requiring user interaction.

NOTE: Before encryption can begin:
After the computer restart, it must be connected to the network.
The client software must have successfully escrowed its encryption keys with the Dell Enterprise Server.

View Encryption Policy and Status

You can view the encryption policy and status on the local computer or in the Dell Remote Management Console.

View Policy and Status on the Local Computer

To view encryption policy and encryption status on the local computer, follow the steps below.

1. Launch *System Preferences* and click **Dell Data Protection**.
2. Click **Policies** to view the current policy set for this computer. Use this view to confirm the specific encryption policies in effect for this computer.

TIP: Click **Refresh** to contact the Dell Remote Management Console to check for policy updates.

The **Policies** pane contains the following information.

General Settings	
Encryption Enabled	*True or Fals*e This is the "master policy" for all other General Settings policies. This policy must be set to *True* for any other General Settings policies to be applied. *True* enables encryption and will initiate encryption for unencrypted volumes, per the *Volumes Targeted for Encryption* or *Encrypt Using FileVault for Mac* policy. False disables encryption and will initiate a decryption sweep for any fully or partially encrypted volumes.
Encrypt Using FileVault for Mac	*True or Fals*e *True* uses FileVault to encrypt the System Volume, including fusion drives. You cannot encrypt volumes other than the System Volume if you choose this policy. If all fixed volumes (which includes the System Volume) must be encrypted, set this policy to *False* and use the *Volumes Targeted for Encryption* policy instead.
Encryption Algorithm	*AES 256 or AES 128* Encryption algorithm used for encrypting Mac volumes.
Volumes Targeted for Encryption	*System Volume Only or All Fixed Drives* *System Volume Only* secures only the currently running system volume. *All Fixed Volumes* secures all Mac OS Extended Volumes on all fixed disks, along with the currently running system volume. This policy and *Encrypt Using FileVault for Mac* cannot be used together. Select either one or the other for encryption.
Workstation Scan Priority	*Highest, High, Normal, Low, or Lowest* This policy specifies the relative priority of the encryption scanning process. High and Highest prioritize scanning speed over computer responsiveness. Low and Lowest prioritize computer responsiveness over scanning speed. Normal balances the two.

Removable Storage	
EMS Encrypt External Media	*True or Fals*e This is the "master policy" for all other Removable Storage policies. This policy must be set to *True* for any other Removable Storage policies to be applied. *True* means that all Removable Storage encryption policies are enabled. *False* means that no encryption of removable storage takes place, regardless of other policy values.
EMS Access to unShielded Media	*Block, Read Only, or Full Access* When this policy is set to *Block Access*, you have no access to removable storage unless it is encrypted. Choosing either *Read-Only* or *Full Access* allows you to decide what removable storage to encrypt. If you choose not to encrypt removable storage and this policy is set to *Full Access*, you have full read/write access to removable storage. If you choose not to encrypt removable storage and this policy is set to *Read-Only*, you can read or delete existing files on the unencrypted removable storage, but the client software will not allow any files to be edited on or added to the removable storage unless it is encrypted.
EMS Encryption Algorithm	*AES 256, Rijndael 256, AES 128, Rijndael 128, or 3DES* Encryption algorithm used to encrypt removable storage.
EMS Data Encryption Key	*Common, User, User Roaming* Although *Common* is available, it is not implemented in this release. Key that is used by the client software to encrypt all data encrypted by EMS.
EMS Automatic Authentication	*Disabled, Local, or Roaming* *Local* automatic authentication allows the encrypted removable storage to be automatically authenticated when inserted in the originally encrypting computer when the owner of that media is logged in. When the *Roaming* key is applied to EMS, Roaming automatic authentication is available when the domain account the user activated with on the Mac computer is the same as the domain account used to provision the removable storage. When automatic authentication is Disabled, users must always manually authenticate to access encrypted media.
EMS Scan External Media	This policy is not yet implemented. Removable storage must be taken to a Windows computer to be scanned.
EMS Access Encrypted Data on unShielded Device	*True or False* *True* allows the user to access encrypted data on removable storage whether the endpoint is encrypted or not. When this policy is *False*, the user will be able to work with encrypted data when logged on to any encrypted endpoint. The user will not be able to work with encrypted data using any unencrypted endpoint.

EMS Device Whitelist	See the AdminHelp for instructions on how to use this policy. This policy allows the specification of removable storage devices to exclude from EMS encryption, thereby allowing users full access to the specified removable storage devices. This policy is available on an Enterprise, Domain, Group, and Endpoint level. Local settings override inherited settings. If a device is in more than one group, all EMS Device Whitelist entries across all Groups, apply. This policy is particularly useful when using removable storage devices that provide hardware encryption. However, this policy should be used with caution. This policy does not check whether removable storage devices on this list provide hardware encryption. Whitelisting removable storage devices that do not have hardware encryption will not have enforced security and will not be protected. Additionally, if a removable storage device is protected by EMS and subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the removable storage device to remove encryption.
EMS Alpha Characters Required in Password	*True or False* *True* requires one or more letters in the password.
EMS Mixed Case Required in Password	*True or False* *True* requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters Required in Password	*1-40 characters* Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	*True or False* *True* requires one or more numeric characters in the password.
EMS Password Attempts Allowed	*1-10* Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	*True or False* *True* requires one or more special characters in the password.
EMS Access Code Attempts Allowed	*1-10* Number of times the user can attempt to enter the Access Code.
EMS Access Code Failure Action	Action to take following unsuccessful Access Code Attempts Allowed: • *Apply Cooldown* to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time Increment policies). • *Wipe Encryption Keys* to have the client software delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to an encrypted computer for which they have a login.
EMS Access Code Required Message	*String - 5-512 characters - Authentication Failed: Please contact your system administrator.* Message that displays when a user needs to contact you for an Access Code (after authentication failure). Message policies must have non-blank values. “Space” and “Enter” characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated in the client software. Dell recommends that you customize the second sentence of the message to include specific instructions about how to contact a Help Desk or Security Administrator for authentication failures.

EMS Access and Device Code Length	*8, 16, or 32* Number of characters Access and Device Codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Cooldown Time Delay	*0-5000 seconds* Number of seconds the user must wait between the first and second rounds of Access Code entry attempts.
EMS Cooldown Time Increment	*0-5000 seconds* Incremental time to add to the previous cooldown time after each unsuccessful round of Access Code entry attempts.
EMS Access Code Failed Message	*String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator.* Message that displays following unsuccessful Access Code Attempts Allowed. Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated in the client software. Dell recommends that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules	See the AdminHelp for instructions on how to use this policy. Encryption rules used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. Storage devices that incorporate multi-interface connections, such as Firewire, USB, and eSATA, may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Mac operating system handles storage devices based on interface type.
EMS Block Access to UnShieldable Media	*True or False* Block access to any removable storage that is less than 20MB and thus has insufficient storage capacity to host EMS (such as a 1.44MB floppy disk). All access is blocked if *Encrypt External Media* and this policy are both *True*. If *Encrypt External Media* is *True*, but this policy is *False*, data can be read from the non-encryptable removable storage, but write access to the media is blocked. If *Encrypt External Media* is *False*, then this policy has no effect and access to non-encryptable removable storage is not impacted.
Shield Permissions	
Policy Proxy Connections	*String - maximum of 1500 characters* Fully Qualified Dell Policy Proxy host names, or IP addresses, separated by carriage returns. When polling for policy updates, the client software will attempt to connect to the Dell Policy Proxy hosts in the order shown until a connection is successful. The client computer's configuration file (com.dell.ddp.plist) may specify additional Dell Policy Proxy host names, which are not listed here. However, the client computer will attempt to connect to the Dell Policy Proxy hosts specified in this policy before those specified in the client software's configuration file.
Policy Proxy Polling Interval	*1-1440 minutes* The interval that the client software attempts to poll the Dell Policy Proxy for policy updates and send inventory information to the Dell Policy Proxy.

User Experience	
Force Restart on Policy Updates	*True or False* *True* forces a computer restart after the specified delay upon receiving a policy update requiring a restart. The delay is specified by the *Length of Each Restart Delay* and *Number of Restart Delays Allowed* policies. *False* neither forces nor prompts for a restart. The policy requiring the restart will take effect the next time the user restarts their computer.
Length of Each Restart Delay	If *Force Restart on Policy Updates* is set to *True*, this value is the number of minutes a user can delay a restart before another restart prompt is displayed. If *Force Restart on Policy Updates* is set to *False*, this policy is ignored. The client software displays the restart prompt for five minutes each time. If the user does not respond to the prompt, the dialog is dismissed and the next delay begins. If the five minute timer expires and no restart delays remain, the computer restarts immediately.
Number of Restart Delays Allowed	If *Force Restart on Policy Updates* is set to *True*, this value is the number of times a user can delay a restart. If this policy is set to "0", the client software prompts the user to restart immediately and will force the restart if the user does not acknowledge the prompt within five minutes. If *Force Restart on Policy Updates* is set to *False*, this policy is ignored.

3 Click **Encryption** to view the status of the volumes targeted for encryption.

State	Description
Excluded	The volume is excluded from encryption. This applies to unencrypted volumes when encryption is disabled, external volumes, volumes with formats other than Mac OS X Extended (Journaled), and non-system volumes when the *Volumes Targeted for Encryption* policy is set to *System Volume Only.*
Preparing volume for encryption…	The client software is currently initiating the encryption process for the volume but has not begun the encryption sweep.
Volume cannot be resized	The client software cannot start encryption because the Volume cannot be resized appropriately. After receiving this message, contact Dell Pro Support and provide the log files.
Needs repair before encryption begins	The volume failed Disk Utility verification. To repair a volume, follow the instructions in Apple Support article HT1782 (http://support.apple.com/kb/HT1782).
Encryption preparation complete. Pending restart…	Encryption will begin after restart.
Waiting to escrow keys with Dell Server…	To ensure all encrypted data is recoverable, the client software will not begin the encryption process until all encryption keys are successfully escrowed to the Dell Enterprise Server. The client software will poll for Dell Device Server connectivity while in this state until the keys are escrowed.
Encrypting…	An encryption sweep is in progress.
Encrypted	The encryption sweep is complete.
Decrypting…	A decryption sweep is in progress.
Restoring to original state…	The client software is restoring the partition scheme to its original state at the end of the "Decrypting..." process. This is the decryption sweep equivalent of the "Preparing volume for encryption" state.
Decrypted	The decryption sweep is complete.

Color	Description
Green	Encrypted portion
Red	Not encrypted portion
Yellow	Portion being re-encrypted For example, by a change in encryption algorithms. The data is still secure. It is just transitioning to a different type of encryption.

The Encryption pane includes all volumes attached to the computer residing on GUID Partition Table (GPT) formatted disks. The volumes can have one of five configurations described below.

Icon	Volume Type and Status
	The currently booted Mac OS X system volume. This volume is shown with a BOOT badge on its volume icon.
	A volume configured for encryption. These volumes are shown with a Dell badge on their volume icons.
	The currently booted Mac OS X system volume that is also configured for encryption. This volume is shown with both a BOOT badge and a Dell badge on its volume icon.
	A volume that does not support encryption. This includes FAT32-formatted volumes. These volumes are shown with a red circle/slash badge on their volume icons.
	A volume excluded from encryption. These volumes are shown with their original Mac OS X volume icons.

View Policy and Status in the Dell Remote Management Console

To view encryption policy and encryption status in the Dell Remote Management Console, follow the steps below.

1. As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left pane, click **Protect & Manage** > **Endpoints**.
3. Enter a filter to search for the endpoint. The wild card character is *. For best results, include non-wild card characters at the beginning of the filter (e.g., User* instead of *ser). You can enter Common Name, Universal Principal Name, or sAMAccountName. You may also leave the field blank to display all endpoints.
4. Click **Search**. An endpoint or list of endpoints displays, based on your search filter.
5. Locate the appropriate endpoint and click the **Details** icon.
6. Click the *Details & Actions* tab.

   The Endpoint Detail area displays information about the Mac computer.

   The Shield Detail area displays information about the client software, including encryption sweep start and end times for this computer.

To view effective polices, in the Actions area, click **View Effective Policies**.

7 Click the *Security Policies* tab. The following tasks can be completed from this tab:

Expand the types of policies as desired. Change individual policies as desired. When finished, click **Save**. In the left pane, click **Actions** > **Commit Policies**. Click **Apply Changes**.

8 Click the *Users* tab. This area displays a list of users activated on this Mac computer. Click the user's detail icon to display the information for all computers this user is activated against.

9 Click the *Endpoint Groups* tab. This area displays all of the endpoint groups to which this Mac computer belong.

User Experience

For maximum security, the client software disables the *Automatic Login* feature of Mac OS X computers.

Additionally, the client software automatically enforces the Mac OS X feature *require password after sleep or screen saver begins*. Lion (and later) enhances this setting by allowing a configurable amount of time in sleep/screen saver mode before enforcing authentication. The client software allows a user to set a value up to five minutes before authentication is enforced.

Users can use the computer normally as the encryption sweep progresses. All data on the currently booted system volume is being encrypted, including the operating system, while the operating system continues to operate.

If the computer is restarted or enters system sleep, the encryption sweep pauses and then automatically resumes after the restart or wake.

The client software does not support the use of hibernation images, which the Mac OS X *Safe Sleep* feature uses to wake the computer if the battery is fully discharged during sleep.

To reduce user impact, the client software automatically updates the system sleep mode to disable hibernation and enforces this setting. The computer can still enter sleep, but the current system state will be maintained only in memory. Therefore, the computer will be fully restarted if completely shut down during sleep, which could occur if the battery runs down or is replaced.

Recovery

Occasionally, you may need access to data on encrypted disks. As a Dell Administrator, you can access encrypted disks without decrypting them, saving you valuable time.

You might need to access a user's encrypted data for many reasons, but a few common use cases are as follows:

- You may need to move a user's encrypted data to a different Mac as part of a hardware refresh.
- You may need to access an encrypted disk because of an operating system fault that causes the system volume to no longer boot, and you need to run various utilities to repair the operating system.
- You may need to access a user's encrypted data because the user made an unauthorized configuration change, and you need to remedy the situation.

This section guides you through the process of using **one** of the three recovery operations available.

Choose **one** option below:

- Mount Volume
- Accept New System Configuration
- FileVault Recovery - use only if using FileVault encryption on the endpoint to be recovered. FileVault can be used with Dell Data Protection | Enterprise Edition v7.4 or later running on Mac OS X 10.7 or later. FileVault recovery is also used on fusion drives.

Mount Volume

Prerequisites

- An unencrypted external recovery volume or computer that will be running the recovery utility
- A FireWire cable
- The Device ID/Unique ID of the computer targeted for recovery - In most cases, you can find the computer targeted for recovery in the Dell Remote Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Unique ID/Device ID is "John Doe's MacBook.Z4291LK58RH".
- The Dell installation media

Process

1. As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left pane, click **Actions** > **Recover Endpoint**.
3. When the Recover Endpoint page displays, select the Endpoint type as Mac from the drop-down menu and enter the **Unique ID**.

TIP: You can access the Unique ID by clicking **Endpoints** in the left pane and clicking **Search**. Select the correct device and click the Device Details icon. The Unique ID displays. Write the Unique ID or type it into TextEdit.

4. To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download**, and click **Save**.

NOTE: If firmware password protection is enabled on this computer, you will be prompted for the firmware password to access the preboot Startup Manager. You can find the firmware password for this computer in the recovery bundle downloaded in step 4. See How to Enable Mac OS X Boot Camp for more information.

5. Boot the target computer from a pre-created external recovery volume. You can accomplish this by either launching the Startup Disk pane in System Preferences and selecting the recovery volume, or by holding down the **Options** key while you restart this computer and selecting the recovery volume in the preboot Startup Manager.

   or

   Boot the computer targeted for recovery into Target Disk Mode. You can accomplish this by either launching the Startup Disk pane in System Preferences and clicking **Target Disk Mode**, or by holding down the **T** key while you restart this computer.

NOTE: Firmware password protection blocks the ability to use the T key at startup to enter Target Disk Mode. More information about Target Disk Mode is available from Apple at http://support.apple.com/kb/HT1661.

   Now connect this computer to the host computer that will perform the recovery operation using a FireWire cable.

6. Mount the Dell-Data-Protection-<version>.dmg.

NOTE: The Recovery Utility must be the same or newer version than the version of client software installed on the computer targeted for recovery.

7. In the Utilities folder located in the Dell installation media, launch the Dell Recovery Utility.

   A message displays stating, "The DDP kext [kernel text] must be loaded in order to modify encrypted disks. Type your password to allow this."

8. Enter the password for the administrator or user.

   A message displays stating, "Needs Install: Recovery needs to install."

9. Click **Install**.
   The *Dell Recovery Utility Select Volumes* dialog displays.

10 Select the volume or drive that needs recovery and click **Continue**.

Selecting the drive will recover all volumes on the drive at once. The file selector window displays.

11 Select the recovery bundle (saved in step 4) and click **Open**.

The *Select Recovery Operation* dialog displays.

12 Select the **Mount Volume** option.

13 Click **Continue** to confirm the *Mount Volume*.

The *Mount Volume Successful* dialog displays.

14 Click **Close**.

You are now able to open a Finder window and access data on the encrypted volume as you would a normal volume. All data will be transparently encrypted and decrypted as files are transferred between the volumes.

Accept New System Configuration

If a firmware password or other system configuration change invalidated the encryption key on an encrypted computer, choose this option to accept the updated system configuration on the next restart and restore access to the computer.

Because encryption is tied to specific device configuration, changes to the configuration invalidate the client software encryption key. When choosing to accept the new system configuration, you simply instruct client software to reset its security based on the new configuration. For example, you may need to move the drive to a different Mac because a user broke the screen. Using this method, you instruct the client software to accept this "new" configuration as valid.

Prerequisites

- An unencrypted external recovery volume or computer that will be running the recovery utility
- A FireWire cable
- The Device ID/Unique ID of the computer targeted for recovery - In most cases, you can find the computer targeted for recovery in the Dell Remote Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Unique ID/Device ID is "John Doe's MacBook.Z4291LK58RH".
- The Dell installation media

Process

1 As a Dell Administrator, log in to the Dell Remote Management Console.

2 In the left pane, click **Actions** > **Recover Endpoint**.

3 When the Recover Endpoint page displays, select the Endpoint type as Mac from the drop-down menu and enter the **Unique ID**.

TIP: You can access the Unique ID by clicking **Endpoints** in the left pane and clicking **Search**. Select the correct device and click the Device Details icon. The Unique ID displays. Write the Unique ID or type it into TextEdit.

4 To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download**, and click **Save**.

NOTE: If firmware password protection is enabled on this computer, you will be prompted for the firmware password to access the preboot Startup Manager. You can find the firmware password for this computer in the recovery bundle downloaded in step 4. See How to Enable Mac OS X Boot Camp for more information.

5 Boot the target computer from a pre-created external recovery volume. You can accomplish this by either launching the Startup Disk pane in System Preferences and selecting the recovery volume, or by holding down the **Options** key while you restart this computer and selecting the recovery volume in the pre-boot Startup Manager.

or

Boot the computer targeted for recovery into Target Disk Mode. You can accomplish this by either launching the Startup Disk pane in System Preferences and clicking **Target Disk Mode**, or by holding down the **T** key while you restart this computer.

NOTE: Firmware password protection blocks the ability to use the T key at startup to enter Target Disk Mode. More information about Target Disk Mode is available from Apple at http://support.apple.com/kb/HT1661.

6 Now connect this computer to the host computer that will perform the recovery operation using a FireWire cable.

7 Mount the Dell-Data-Protection-<version>.dmg.

NOTE: The Recovery Utility must be the same or newer version than the version of client software installed on the computer targeted for recovery.

8 In the Utilities folder in the Dell installation media, launch the Dell Recovery Utility.
A message displays stating, "The DDP kext [kernel text] must be loaded in order to modify encrypted disks. Type your password to allow this."

9 Enter the password for the administrator or user.

A message displays stating, "Needs Install: Recovery needs to install."

10 Click **Install**.

The *Dell Recovery Utility Select Volumes* dialog displays.

11 Select the volume or drive that needs recovery and click **Continue**.

Selecting the drive will recover all volumes on the drive at once.

The file selector window displays.

12 Select the recovery bundle (saved in step 4) and click **Open**.
The *Select Recovery Operation* dialog displays.

13 Select the **Accept new system configuration** option.

14 Click **Continue** to confirm *Accept New System Configuration*.

15 Enter your password to reset ownership and accept the new system configuration.

16 Click **OK**.

A *Recovery Complete* message will appear when booted to the original internal system volume. This message will prompt you to restart the computer again. The client software has now accepted the updated system configuration, and you can access your computer normally.

FileVault Recovery

Recovery of a managed FileVault-encrypted volume is significantly different from recovery of a Dell-encrypted volume. The recovery process is dictated by Apple and is automated where possible but requires a few more steps.

Prerequisites

- An unencrypted external recovery volume or computer that will be running the recovery utility
- A USB drive
- A Firewire cable
- The Device ID/Unique ID of the computer targeted for recovery - In most cases, you can find the computer targeted for recovery in the Dell Remote Management Console by searching for the owner's user name and viewing the devices encrypted for that user. The format of the Unique ID/Device ID is "John Doe's MacBook.Z4291LK58RH".
- The Dell installation media

Process

1. As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left pane, click **Actions** > **Recover Endpoint**.
3. When the Recover Endpoint page displays, select the Endpoint type as Mac from the drop-down menu and enter the **Unique ID**.

TIP: You can access the Unique ID by clicking **Endpoints** in the left pane and clicking **Search**. Select the correct device and click the Device Details icon. The Unique ID displays. Write the Unique ID or type it into TextEdit.

4. To save the recovery bundle to your USB, click **Download**, and click **Save**.
5. Boot the target computer from a pre-created external recovery volume. You can accomplish this by holding down the **Options** key while you restart this computer and selecting the recovery volume in the pre-boot Startup Manager.
6. Mount the Dell-Data-Protection-<version>.dmg.

NOTE: The Recovery Utility must be the same or newer version than the version of client software installed on the computer targeted for recovery.

7. In the Utilities folder located in the Dell installation media, launch the Dell Recovery Utility.
   The *Dell Recovery Utility Select Volumes* dialog displays.
8. Select the FileVault volume to recover and click **Continue**.
   The *Choose Recovery Bundle* dialog displays.
9. Select the recovery bundle (saved in step 4) and click **Open**.
   The *File Vault Recovery Instructions* dialog displays.
10. Read the instructions and click **Continue**.
    The *Confirm Recovery Operation* dialog displays.
11. Highlight the FileVault volume to recover and click **Continue**.

    The file selector window displays.
12. Navigate to your USB drive as the location to save the files and click **Open**.
    The *Recovery Operation Results* dialog displays, indicating the files have been created.
    SUCCESS will be the status next to the volume name.
    After outputting the files to the USB drive, this program displays the **exact** commands you will need to run from the recovery volume to mount or decrypt the FileVault volume.
13. Copy the command strings shown on the final *Recovery Operation Results* dialog.
14. Boot to the OS Recovery Volume by holding down the Option key and using the boot picker.
    After the OS Recovery Volume is accessed, the *Mac OS X Utilities* dialog displays.
15. Select **Utilities** > **Terminal** from the *Tools* menu.
16. **To Mount the volume:** In Terminal, type the full path to the USB and script name **fv2mount.sh** to mount the volume so you can copy files from the Terminal or image the disk from Disk Utility. For example, /CRUZER/fv2mount.sh.

    To decrypt the volume: In Terminal, type the full path to the USB and script name **fv2.decrypt.sh** to decrypt the volume, allowing you to do anything with this volume as you would with any other volume. For example, /CRUZER/fv2.decrypt.sh.
17. Reboot the computer.

The computer can now be used normally.

Uninstall Dell Data Protection | Enterprise Edition for Mac

The client software may be uninstalled by running the **Uninstall Dell Data Protection** application. To uninstall the client software, follow the steps below.

NOTE: Before running the uninstall application, the disk must be fully decrypted.

1. If the disk is currently encrypted, set the computer's **Encryption Enabled** policy to **False** in the Dell Remote Management Console and commit the policy.

   If the Mac is running either OS X Mountain Lion or Mavericks, a dialog displays to ask for access to System Preferences and control of the computer so that the client software can decrypt the disk.

   a. Click **Open System Preferences**.

      If **Deny** is selected, the uninstallation and decryption are unable to continue.

   b. Enter the administrator password.

2. After the disk is fully decrypted, restart the computer (when prompted).
3. After the computer restarts, launch the **Uninstall Dell Data Protection** application (located in the Utilities folder in the Dell-Data-Protection-<version>.dmg file in the Dell installation media).

   Messages display the status of the uninstallation.

Dell Data Protection | Enterprise Edition for Mac is now uninstalled, and the computer can be used normally.

4

Activation as Administrator

The Client Tool offers the administrator new methods for activating the client software on a Mac computer and examining the client software. Two methods of activation are available:

- Activation using Administrator credentials
- Temporary activation that emulates the user without leaving footprints on that computer.

Both methods can be used directly through a shell, or in a script.

WARNING: Do not activate the client software on more than five computers with the same network account. Serious security vulnerabilities and degraded performance of your Enterprise Server/Enterprise Server - VE could result.

Prerequisites

- DDP|Enterprise Edition for Mac 8.1.3 or later must be installed on the remote computer.
- Do not activate through the client user interface prior to attempting to activate from a remote location.

Activate

Use this command to activate the client as administrator.

Example:

client -a *username@domain.com password admin admin*

Activate Temporarily

Use this command to activate the client without leaving footprints on the computer.

1. Open a shell or use a script to activate the client software:

   client -at *username@domain.com password*

2. Use the Client Tool to retrieve information about the client software, its policies, disk status, user account and more. For more information about the Client Tool, see Appendix D: Client Tool.

NOTE: After activation, information about the client software, including policies, disk status, and user information, is also available in System Preferences in the Dell Data Protection preferences.

Appendix A

About Optional Firmware Password Protection

NOTE: More recent Mac computers do not support Firmware Password Protection. Firmware Password Protection is supported for the following models:
iMac11.*
Macmini4.*
MacBook7.*
MacBookAir2.*
MacBookPro7.*
MacPro5.*
XServe3.*
For example, iMac11.1 and iMac11.2 will support Optional Firmware Password Protection (as indicated by the *), but iMac12.1 or later will not.

NOTE: When the FirmwarePasswordMode key option is set to **Optional**, it only disables client enforcement of firmware password protection. It does **not** remove any existing firmware password protection. You can remove any existing firmware password using the Mac OS X Firmware Password Utility.

If you intend to use Boot Camp (see How to Enable Mac OS X Boot Camp for instructions) on encrypted Mac computers, you **must** configure the client to **not** use firmware password protection.

Mac computers use firmware password protection to enhance access security of the computer. On Mac computers, by default, the protection is turned *OFF*. During client installation, whether a new installation or an upgrade from an earlier client version, you have the ability to edit the existing com.dell.ddp.plist file to allow the *FirmwarePasswordMode* key to be set to either *Required* or *Optional*. The *Required* option is the default setting that enforces firmware password protection, while the *Optional* setting causes the firmware password to not be enforced. Following the installation or upgrade, the client evaluates the modified installer com.dell.ddp.plist file during restart.

NOTE: To prevent users from changing the computer's security posture, the client does not accept changes to the FirmwarePasswordMode key after installing the client software.
You can change the value of this key after installation or upgrade by initiating a disk decryption process, and then re-enabling encryption.

If you want Mac OS X firmware password protection to be **required**, follow normal client installation/upgrade procedures outlined in Install/Upgrade Dell Data Protection | Enterprise Edition for Mac.

B

Appendix B

How to Enable Mac OS X Boot Camp

NOTE: When using Boot Camp, the Windows operating system cannot be encrypted.

Boot Camp is a utility included with Mac OS X that assists you in installing Windows on Mac computers in a dual-boot configuration. Boot Camp is supported with the following Windows operating systems:

- Windows 7 and 7 Home Premium, Professional, and Ultimate (64-bit)
- Windows 8 and 8 Pro (64-bit)

To use Boot Camp on encrypted Mac computers, you must configure your client installation to **not** use firmware password protection. See the Command Line Installation/Upgrade for instructions.

The following Boot Camp configurations are supported:

- Mac OS X v10.7 Lion with Boot Camp v3.1 or later
- Mac OS X v10.8 Mountain Lion with Boot Camp v3.1 or later
- Mac OS X v10.9 Mavericks with Boot Camp v5 or later

If Windows XP is installed on an NTFS partition, the Windows XP boot configuration must be manually updated before the client encrypts or decrypts the Mac OS X system volume.

NOTE: You must ensure Windows is installed before deploying client policies enabling encryption. After the client begins the encryption process, it disallows disk partition operations required by Boot Camp.

Use the following steps to update the Windows XP boot configuration on NTFS partitions. Failure to do so will cause the Windows boot process to fail until this update is performed:

1. Restart the computer to Windows XP.
2. Open C:\boot.ini.
3. Change the partition identifiers from 3 to 4. See example below:

   ```
   [boot loader]
   timeout=30
   default=multi(0)disk(0)rdisk(0)partition(4)\WINDOWS
   [operating systems]
   multi(0)disk(0)rdisk(0)partition(4)\WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect
   ```

4. Restart the computer to Mac OS X.
5. Begin the encryption process.

NOTE: Restore the Windows boot configuration to its original values before completing a decryption operation.

C

Appendix C

How to Retrieve a Firmware Password

Even if the client computer is configured for firmware password enforcement, it may not be needed for recovery. If the computer to recover is bootable, set the boot target in the Startup Disk system preferences pane.

In the case where the firmware password is needed to accomplish recovery (if the computer is not bootable and firmware password protection is enforced), follow the steps below.

To retrieve a firmware password, you must first retrieve the recovery bundle containing the disk's encryption keys.

1. As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left pane, click **Actions > Recover Endpoint**.
3. When the Recover Endpoint page displays, select the Endpoint type as Mac from the drop-down menu and enter the **Unique ID**.

TIP: You can access the Unique ID by clicking **Endpoints** in the left pane and clicking **Search**. Select the correct device and click the Device Details icon. The Unique ID displays. Write the Unique ID or type it into TextEdit.

4. To save the recovery bundle to the external recovery volume or computer that will be running the recovery utility to perform the recovery operation, click **Download**, and click **Save**.
5. Open the recovery bundle to retrieve the firmware password for the computer targeted for recovery. The firmware password is located within the string tags after the **FirmwarePassword** key.

   For example: <key>FirmwarePassword</key>
   <string>Bo$vun8WDn</string>

D

Appendix D

Client Tool

The Client Tool is a shell command that runs on a Mac endpoint. It is used to activate the client from a remote location or to run a script through a remote management utility. As administrator, you can activate a client and do the following:

- Activate as administrator
- Activate temporarily
- Retrieve information from the Mac client

To use the Client Tool manually, open a ssh session and enter the desired command on the command line.

Example:

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Enter **client** alone to display the usage instructions.

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client**

Client Tool Commands

Command	Purpose	Syntax	Results
Activate	Activates a Mac client .	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword	0 = Success 2 = Activation failed, and reason for failure 6 = User not found
Activate temporarily	Activates a Mac client without leaving a footprint.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Disk	Request the status of the disk	-d	Disk status displays, including the disk's ID, encryption status, and policies If empty braces are returned, it means no disks are encrypted.
Policy	Request the policies of the Mac client	-p	Policies display

Client Tool Commands

Command	Purpose	Syntax	Results
Server	Polls the server for updated policies on behalf of the Mac client **NOTE:** The poll can take several minutes to complete.	-s	0 = Success Any other value indicates that either the server or Mac client software was busy or not responding.
Test	Test the Mac client's activation status	-t localAccount*	0 (domainAccount) = Success 1 = Not activated 6 = User not found
User	Request user information	-u localAccount*	The user's account information displays: 0 (account information) = Success 6 = User not found
Version	Request the Mac client's version	-v	The version of the Mac client displays: Example: 8.x.x.xxxx

* The Client tool's account is used for the localAccount unless another is specified.

The Plist Option

The -plist option prints the results of the command with which it is combined. It follows the command and must appear prior to its arguments to make the results print as a plist.

Examples

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -p -plist**

To retrieve the policies from the client and print them.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

To temporarily activate the client and print the result.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -s ; echo$?**

To poll the server for updated policies on behalf of the client and display them on-screen.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -d -plist**

To retrieve the client's disk status and prints it.

Global Return Codes

No error	0
Parameter error	4
Unrecognized command	5
Socket timed out	8
Internal error	9

Glossary

Dell Device Server - The Dell Device Server is used for client activations. The Dell Device Server is a component of the Dell Enterprise Server.

Dell Enterprise Server - The Dell Enterprise Server is made up of a collection of components. When referring to the Server-side of the product as a whole, it is collectively known as the Dell Enterprise Server.

Dell Policy Proxy - The Dell Policy Proxy is used to distribute policies to Dell Data Protection | Enterprise Edition for Mac client software. The Dell Policy Proxy is a component of the Dell Enterprise Server.

Dell Remote Management Console - The Dell Remote Management Console is the administrative console for the entire enterprise deployment. The Dell Remote Management Console is one component of the Dell Enterprise Server.

Shield - Occasionally, you may see this term in the documentation and in the client user interface. “Shield” is a term used to represent the client software.

0 XXXXXA0 X